UNIVERSITY OF ILLINOIS

May 7 1992

THIS IS TO CERTIFY THAT THE THESIS PREPARED UNDER MY SUPERVISION BY

Sean Michael Higgins

ENTITLED Analyzing the Wartime Initiative of Allied Scientists at Penetrating the German Enciphering Machine Known as "Enigma"

IS APPROVED BY ME AS FULFILLING THIS PART OF THE REQUIREMENTS FOR THE DEGREE OF Bachelor of Arts in History and Philosophy of Science

Instructor in Charge

APPROVED: Richard W Burkhardt

HEAD OF DEPARTMENT OF Humanities

O-1364

Analyzing the Wartime Initiative of Allied Scientists At Penetrating the German Enciphering Machine Known as 'Enigma'

by

Sean Michael Higgins

Thesis

for the
Degree of Bachelor of Arts
in
History and Philosophy of Science

College of Liberal Arts and Sciences
University of Illinois
Champaign, Illinois

1992

Table of Contents

Soon after the conclusion of World War Two, the historical annals began, explaining how the Allied forces defeated Nazi Germany. Additional, highly classified wartime material has also been written into history after the expiration of the thirty year rule. Nevertheless, there still remains one wartime secret which has not been released. It is quite probable that this secret may never be fully divulged and that its official history will never be completely documented. It is the role Polish, French and British scientists played while working secretly with the military; specifically their method of penetrating the German enciphering machine now known as "Enigma." Over the six years of war, it is estimated that nearly ten thousand men and women worked secretly on breaking the German military ciphers. This intellectual mass was formed as a special adjunct of the British Code and Cipher School. The cover name for the department was Room 47, The Foreign Office, London. Moreover, the great importance for secrecy and also for fear of bombing necessitated the relocation of this group to a small town in Buckinghamshire called Bletchley, where a collection of wooden huts surrounded a large Victorian mansion known as: Bletchley Park (Whiting, p.44).

The wartime activity at Bletchley and its outposts was the most closely guarded secret of the war (Cave Brown, p.150). This secret was well kept until thirty-one years after the war had ended that a retired Royal Air Force Intelligence officer, F.W. Winterbotham, wrote The Ultra Secret. This book revealed for the

first time the exact nature of British wartime codebreaking and some of the consequences it had on the course of the war. It was not until October 1977, when the Official Secrets Act expired, that the Public Records Office in London released the texts of thousands of deciphered Enigma messages(Bennett, p.405). Prior to these revelations, one would have been lucky to find in the archives even the slightest reference to either "Enigma" or "Ultra."

Enigma was the name of the first device that the Germans used for the enciphering of their messages; later in the war similar but more complex machines were developed which added to the maze of encrypted messages. "Ultra" was the British code-name for the intelligence which was derived from Enigma and the other machine ciphers used during the war.

The science of cryptography has a long and distinguished history. Almost as soon as humans learned to write, they devised ways to keep their messages secret; for example, enciphered writing is mentioned in Greek works such as the Iliad and even in The Old Testament. Julius Caesar often encrypted messages, substituting letters three places farther on the alphabet, to deceive enemies. Mary Queen of Scots was ordered beheaded after Queen Elizabeth's chief spy intercepted and decoded Mary's letters, which revealed that she was plotting against Elizabeth(Time, p.55). The Arabs developed cryptography during the Middle ages but the real turning point for cryptography occurred with the invention of the telegraphic code by Samuel Morse in 1844 and with the

establishment of dependable long-distance wireless telegraphy around the turn of the century (Kahn, 1967, pp.71, 93, 189).

The wire telegraph enabled military commanders to keep in touch with their forward units and in turn required special signal corps to be formed for this purpose. Enemy agents soon discovered that the wire telegraph could easily be tapped, so codes were devised to prevent the messages from being read. The telegraph had many limitations. It was a very cumbersome unit, only usable in a static war where wires could be laid and it was clearly not viable to communicate with naval ships at sea(Kahn, 1967, p.88).

The invention of wireless telegraphy greatly reduced these limitations; now military or naval units could be contacted at almost any distance and two-way instantaneous traffic be initiated (Winterbotham p.9). All this was at the cost of such traffic being available to an enemy who simply required a suitable receiving set (tuned into the proper frequency) in the safety of his own territory. Nonetheless, the advantages of mobility and simplicity gained by use of the wireless telegraph far outweighed its disadvantages. As a result, the use of military and diplomatic messages via the wireless telegraph multiplied during the First World War. Knowing that the enemy would be listening though, required the sender of messages to use secret codes and ciphers on a massive scale. In turn, code-breakers (cryptanalysts) came on the scene, perfecting their skills on the plethora of signals which were so easily accessible. (Kahn, 1967, pp.189-92)

During the First World War, the British managed to cut Germany's transatlantic cable (Kahn, 1967, pp.348-50). This forced the Germans to send most of their diplomatic traffic to the Americas by wireless, to which the British intercepted. These messages were decoded by a team working in Room 40 of the Admiralty building. As the war continued, Room 40 penetrated German codes with the aid of a German naval codebook which was salvaged from a cruiser that had sunk in the Baltic seas. One of the greatest achievements by this team was in solving the intercept of the "Zimmerman" telegram, which was greatly responsible in bringing the United States into the war upon its disclosure (Kahn, 1967, p.266; Whiting, p.43).

After the war, the wartime work of Room 40 was made public in Britain and undoubtedly noted elsewhere. It was apparent that the type of codes used during the war, which relied on the substitution of words or phrases by code-groups of letters, could, however large, eventually be compromised. The reason was simply repetition. Given sufficient messages in a certain code, the cryptanalysts could later reconstruct the code and recover the original text from known phrases (Kahn, 1967, p.381). Additionally, forms of address such as "Field Marshall," "To Commanding Colonels," or even "Good luck," would provide a key. There was also the possible danger that codebooks would fall into enemy hands (Winterbotham, p.8). Moreover, the sheer volume of military traffic posted an almost insuperable problem of logistics

in the drawing up, printing and distribution of thousands of different codebooks. There was also the time-consuming and redundant process of encoding and decoding the messages which was not practical for a military unit under fire.

The history of cryptography took a dramatic leap forward with the work of an American, Edward Hebern (Lewin, p.34) In 1915 he had become fascinated by cryptography and devised a simple machine-generated code based on the then very new electrical typewriter. The keys were, in reality, switches When an 'A' was pressed, an electric circuit was completed, current flowed to an electromagnetic actuator, and a mechanical-type hammer printed the letter 'A' Hebern simply rearranged the wiring so that the 'A' key printed, for example, 'R' and an 'L' was 'S', and so on. As a result, a message read 'Send Ammo' would possibly print as 'LTWG RJJU'. The importance of this early electromagnetic enciphering was its simplicity of operation, for, with the addition of suitable switching circuits, 'LTWG RJJU' could be then typed out to print the original plaintext 'Send Ammo'. The machine was reversible and very quick, encoding and decoding took no longer than the time needed to type the message. The messages encoded by Hebern machines could be transmitted by Morse code to a ship at sea and typed on to an identically-wired typewriter, which would easily decode them and in turn encode a reply.

The codes generated by Hebern typewriters are those known as "mono-alphabetic substitution" and, although secure from casual

readers, would not pose a half-way competent cryptanalyst any difficulty in their breaking (Kahn, 1983, p.57). The codebreaker, given such a message of reasonable length, would make a frequency analysis of the letters or figures of the encoded text. All western languages have a characteristic repetition rate of letters whatever the content of the text. The order of letter repetition of English is. e,a,o,i,d,h,n,r,s,t,u,y,c,f,g,l,m,w,b,k,p,j,v,q,x,z (Kahn, 1967, pp.381-2).

Letter-frequency analysis is the foundation upon which crytanalysis is based. It would not take the codebreaker long to penetrate a simple substitution cipher, for 'e' is by far the most common letter in English. Vowels would soon be recovered, as would key consonants and before long enough of the plaintext would be deciphered to enable the gaps to be filled from the sense of the message.

To avoid the characteristic 'give away' of the letter frequency, it would be necessary to change the encoding so often that frequency analysis would be impossible, or at least very difficult. Hebern was aware of this and in 1917 began to experiment with a second encoding machine using rotors which switched the connections of his electric typewriter each time a key was pressed, thus changing the entire code alphabet (Van der Rhoer, p.55). After much work he produced his 'Electric Code Machine', U.S. Patent 1,683,072. Later, in 1928, Hebern even

managed in selling some of them to the U.S. Navy (Kahn, 1967, pp.415-16).

Although the machine looked like a typewriter, it was definitely not. It did not type anything but it had a keyboard with just twenty-six upper case letters arranged in the same order as a commercial typewriter keyboard. Above the keys on a sloping panel there were twenty-six letters printed on small glass windows, each with an illuminating bulb behind it, again arranged in the same order as a regular keyboard. On the top of the machine, in the position that the rotor and paper would occupy on a standard typewriter, there were five rotors arranged parallel to the keyboard. Each rotor had twenty-six letters of the alphabet engraved on its circumference and each could be preset against an engraved datum. (Kahn, 1967, pp.417-20)

Each rotor was made of insulated material and had twenty-six contacts on either face, one for each letter. The contacts were wired together in pairs in a definite pattern, each of the five rotors having a different wiring (Kahn, 1967, p.411). It was this internal wiring which performed the actual enciphering. The operation of only a single rotor, might look like the following example: if the 'A' key was pressed an electric current flowed via a spring contact brush to the 'A' contact on the first rotor, through the rotor's internal wiring, to emerge on the other side as, say 'R', lighting up the 'R' window on the front of the machine. If 'A' were pressed again, the rotor would advance one letter and the contact

would pass the current via its wiring to, say, the 'H'. Then 'H' would light up on the front panel. Therefor, even a single rotor would provide twenty-six completely different cipher alphabets. Hebern's machine had five such rotors wired in series; when rotor one had made a complete revolution, rotor two moved forward one letter, when it had made a complete revolution, three advanced one letter; and so on. As a result, the Hebern five-rotor machine could generate nearly 12,000,000 different cipher alphabets, which is roughly twenty-six to the fifth power (Kahn, 1967, p.420).

To operate the Hebern machine, one needed to set up a 'maincode' which is a definite starting order for the five rotors, for example 'TBHWL', which would subsequently determine which of the ciphers was used first. As the plaintext was tapped out on the keys the code-letter equivalents would appear in the windows, to be copied down be a second cipher clerk. Deciphering was accomplished by setting up the same maincode TBHWL. The cipher text would then be typed on the keys, with the plaintext appearing by letter in the windows. The Hebern machine had a great level of security due to the enormous number of cipher alphabets produced by the rotors. The question of frequency counts became a 'non-issue'. The time taken to break a Hebern code would have been so long as to render the intercepts useless, certainly during wartime.

Though it appears that Hebern's rotary machine was the first manufactured, it was not the only one to be conceived. In 1919 patent No. 10,700 was taken out by Hugo Alexander Koch of Delft

for a cipher machine which he called 'Geheimschrijfmachine': secret-writing machine (Kahn, 1967, p.402; Whiting, p.40). Koch did not actually construct his invention; but in all events, a German engineer named Arthur Scherbius, bought the patent rights and made the machine, renaming it 'Enigma'-a puzzle. Scherbius's machine was essentially similar to Hebern's, though they seem to have been arrived at independently. The machine had three rotors, but the the third drum reflected the circuit back through the other two, giving the equivalent of six rotors. This, however, was achieved at the cost of never being able to cipher a letter as itself. That is, an 'A' typed would never appear as an 'A' in the encoded message. This was a seemingly small defect, but one which proved to be a serious weakness later

By 1923 Scherbius had his Enigma in production in his Berlin workshops and it was placed on public exhibition at the International Postal Union Congress and the Leipzig Trade Fair, where it was offered as an inexpensive, reliable means of safeguarding commercial cables and telegrams (Whiting, p.41). Although Scherbius was making an auspicious start to his venture, he was unknowingly attracting the attention of others outside the purely commercial and public realm. Discreet enquiries were made and the machine was withdrawn from the exhibition to reappear in the Berlin 'Chiffrierabteilung', the Cipher Department of the Reichswehr. This was the small army permitted to the Germans

under the provisions of the Treaty of Versailles. The head of the department was Colonel Erich Fellgiebel. (Kahn, 1967, p.420-24)

After Fellgiebel's examination, the Enigma machine was totally withdrawn from the commercial market. Its production continued, with significant improvements, but now solely for the German war machine. The arrival of the Enigma had been timely, for Germany was in political and economic turmoil, and the first stirrings of the Nazi party under Adolf Hitler were apparent. In November of 1924, Hitler published his frightening declaration titled, Mein Kampf , my struggle. By the time Hitler had assumed power in Germany in 1933, Staff studies had already begun to sketch their ideas for a new form of warfare, termed Blitzkrieg-lightening warfare-a war of total mobility. This radical concept integrated massive motorized columns and armour, supported by a tactical air force; its successful deployment required fast, reliable communications that could only be furnished by radio. Enigma's, which were lightweight, battery-powered and rugged enough to be operated in the back of army signals trucks on the move, proved ideal (Whiting, p.9).

The Enigma that was issued to the German armed forces had initially three rotors and a plugboard that could make a final superencipherment (Bennett, p.400). German military officers apparently believed that its messages would be completely indecipherable to an enemy without an identical Enigma machine; and even with a captured Enigma, the enemy would have to know the

current 'maincode' used to set up the machine, to break the code; an act which they believed, required an ability that few cryptographers possessed. As it turned out, their assessments were overly optimistic, for the initial secrets of Enigma had already been penetrated (Winterbotham, p.11).

The Poles, surrounded as they were by powerful potential enemies, had, between the wars, developed one of the most efficient Intelligence Services in the world. Their code and cipher bureau,BS4, based in Warsaw, had achieved some remarkable successes, including the breaking of the Russian codes used in the Battle of Warsaw in 1920 (Calvocoressi, pp.31-3). After this early success, the Poles broke the German Reichswehr ciphers, which they read without difficulty until a certain date in 1928, when a new cipher began to be used which the BS4 cryptanalysts suspected was mechanically generated and which they could not break. Soon after, BS4 realized that the source of the cipher that they could not read was some type of advanced copy of Scherbius's commercial Enigma. Fortunately, Polish intelligence officers had seen the commercial Enigma when it was on public exhibition and obtained a rough understanding of its function. It was therefore vital that an example of the military Enigma be procured.

The account of how the first Enigma was truly obtained changes from source to source or differs from various books on the subject. One story explained by Sir William Stephenson in his biography, A Man Called Intrepid, explains how the Polish

underground attacked a German convoy; obtained an actual military Enigma; replaced a typewriter in its place; and blew up the military truck, so as to appear that the Enigma was destroyed in the attack. If accurate, it appears that the deception worked, but most historians regard Stephenson's biography as more of a "history-fiction" than a true historical account. Therefor, while believable, this story should, nevertheless, be taken with a grain of salt.

Another such account, which is believed to be accurate, was told by a Polish ex-Signals officer. The story states that on a Friday afternoon, sometime in 1929, an official from the German legation in Warsaw began to make urgent enquiries at the Railway Parcels Customs Office regarding a packing case consigned to the Legation from the Foreign Office in Berlin. He demanded that it be cleared through Customs immediately, and such was his anxiety that the Poles became suspicious, and thinking (correctly) that a mistake might have been made in Berlin and that something had been sent by ordinary freight that should have been transported in the Diplomatic Bag. The story explained that the persistent German official was informed that the parcel had not yet arrived and that the Customs Office was about to close for the weekend. (Kozaczuk, pp.16, 25-31)

The Customs officers then contacted Polish Military Intelligence, who lost no time in opening the case. In the box was a brand-new military Enigma. Over that weekend, experts from BS4

examined the machine thoroughly before it was skilfully repacked, to await collection by the Germans on Monday (Ibid, p.34).

The examination of the Enigma gave the Poles valuable information; in particular, the internal wiring of the three rotors, and also the addition of the plugboard (called a Stecker by the Germans), which provided a final superencipherment (Bennett, p.400). It was clear that the military Enigma was an advance on the civil version and it was obvious that to keep pace with its developments, exceptional cryptanalysts would be required, involving advanced techniques in higher mathematics. BS4 therefore recruited three brilliant young mathematicians from Poznan University, a German-speaking region of Poland (Bennett, p.401; Kozaczuk, pp.1-8).

One of the trio, Marian Rejewski, had a remarkable analytical mind; moreover, he had been sent to Gottingen University in Saxony for post-graduate training in most recondite higher mathematics pertaining to group and permutation theory and statistics, an essential skill for cryptanalysts (Kozaczuk, pp.4,12) The second member, Jerry Rozycki, was very different and would be able to offer brilliantly imaginative solutions to problems (Ibid, 4,12). The third, Henryk Zygalski, complemented the other two. He was a diligent, steady tinkerer, capable of exploring every possible avenue tirelessly (Ibid, 4,9,12). In 1932, after four years of training, they began work with BS4 on the Enigma intercepts. They were to begin breaking the codes in approximately four and a half

months. This was a remarkable achievement, even though they did receive outside help. This assistance came from the French Service Renseignements-Intelligence Service (Kozaczuk, p.279). They were able to supply BS4 and the trio with certain information, from a German informant, on ciphers, including documents relating to the secrets of the Enigma machine.

When the Poles broke Enigma in 1934, the German code clerks were simply setting the three drums according to a prearranged schedule, as set out in the Army cipherbook, copies which the French Intelligence had previously obtained. However, from the moment that Enigma became general in the German forces, the machine was constantly redeveloped. To continue to read the ciphers, more than purely mathematical techniques were required. BS4 came to the conclusion that several copies of the current Enigma were essential if they were to be able to continue to crack the German messages.

The Polish copies were based on the known commercial model, with the additions which the examination of the Enigma in Warsaw Customs had revealed, and aided by mathematical analysis. The actual machines were built under conditions of great secrecy at the AVA telecommunications factory in Warsaw and were used by BS4 from 1934 (Kozaczuk, pp.25-28). They worked well for a time, but in October of 1936 the Germans began making changes. The superencipherment plugboard was enlarged. In 1937 the 'reflecting' rotor wiring was altered and the keys, that is the

initial setting of the three rotors, were no longer copied from a book; instead, a 'repeated indicator' technique was used. Now the codebook gave the operators the plugboard connections and the rotor settings , which was achieved by twisting the outer ring of the rotors, on which the twenty-six letters of the alphabet were engraved. Each of the three rotors would be differently set Having done this, the operator would place the rotors in the machine and set up the 'ground setting', that is the key or starting position of the three rotors as they appeared in the rotor windows on the top of the machine. The 'ground setting' key would be dependent on the radio 'net' (or frequency) of the sender; these would be different for each unit and would be changed every month pre-war, or three times a day during the war (Kozaczuk, p 29-31).

The following is an example of this process suppose that the 'ground setting' key was 'AAA' an obvious combination, but one that will be used for clarity in this example The operator, having set the key, would then choose at random three letters, and repeat them: SOXSOX (Bennett, p.401). This might be encoded by the Enigma as WRJKBT. The operator made note of this, then set the three rotors to SOX and encode the message by tapping out the plaintext on the Enigma's key's. As he did so, a second cipher clerk noted down the cipher text in five-letter groups When the encoding was complete, the message would be sent by radio in Morse code. The signal would begin by identifying the sender and the recipient by their radio call-signs; the message would start

with SOXSOX and then continue with the five-letter groups of the enciphered text. When the entire message was received, it would be passed to the code clerk for decipherment. He would obtain the plugboard connections, the rotors and key of the net,'AAA', from his codebook; he would then tap out 'WRJKBT' on his Enigma. This would decode as SOXSOX, the three random letters (repeated twice) that the encoding clerk had used. SOX would then be set up on the three rotors and the enciphering text tapped out on the keyboard with the German plaintext emerging letter by letter in the illuminated windows, and subsequently taken down by a second clerk (Bennett, p.400).

To enable the cryptanalysts of BS4 to recover the Enigma ciphers, the Poles built an electro-mechanical device which Rozycki named a 'bomba' (Kozaczuk, pp.53-61). The machine ran through all the possible settings of the three drums until settings were found which deciphered the message on the Polish built copies of Enigma. Precisely how they worked is not altogether clear, but they produced results, though they had certain drawbacks. In the first place, they were expensive to construct, and one bomba was required for each rotor setting; because of the reflection through the rotors, six bombas were needed for a given Enigma key. Secondly, they did not perform the entire operation; there was a complementary aid known as 'the light table'. This was, as the name implies, an illuminated table on which large perforated sheets of card were placed, one on top of another; they

were then manipulated in a certain way until holes appeared where registration occurred, which represented possible drum settings (Kozaczuk, p.237).

The Polish cryptanalysts of BS4 were able to improve their techniques, reaching a peak in the first six months of 1938 as German military traffic increased almost daily. However, their remarkable achievements came to an end in December of 1938. On this month, Germany issued each Enigma machine with two additional rotors, so that the three operational rotors were now selected from five (Calvocoressi, p 26) Since each rotor setting required a bomba, the additional rotors increased the number of bombas needed by a factor of ten, from six to sixty, and of course a highly trained staff to operate them. The Poles of BS4 simply did not have the time or the resources available from their peacetime budget. The Enigma traffic was once more unreadable (Ibid, p.34-6).

Fortunately, a French intelligence officer, Captain Bertrand,had foreseen, at least in part, that the Poles would be in need of help. Just before the appearance of the two extra rotors, he approached the British with a proposal that they should co-operate with the French (Kozaczuk, p.16). The British Secret Service, which is one of the most withdrawn of all clandestine organizations, was to say the least indecisive; but in the inevitability of a new war with Germany in the not so distant future, the suggestion was not entirely dismissed (Kozaczuk,

p.207). Encouraged, the Captain Bertrand sent Britain samples of their intelligence documents and also hinted at the Polish success in penetrating certain German ciphers, by the use of advanced cryptanalytic techniques.

Subsequently, a meeting was set up between representatives of the comparable intelligence services of the Polish, French and British (Bennett, p.401; Kozaczuk, p.56). The meeting began with the Polish revealing the extent of their penetration of Enigma and the problem posed by the German's introduction of the additional rotors. A long discussion followed and two possible courses of action emerged. The first, put forward by a representative of the French Intelligence, was that a 'deception gambit' should be played, involving the idea that the Germans would be supplied with information, through their contacts, that the five-rotor Enigma ciphers were 'blown'. The French argued that the Germans would then drop the system as insecure. However, even if this succeeded, it would only be temporary, for the Germans would hardly drop all ciphers and a new improved form of Enigma would inevitably appear.

The Polish took the position that a better course of action would be a new tripartite effort to break the five-rotor cipher. This alternative was adopted by the representatives and the three intelligence services agreed upon the following: 1. The Poles would continue their mathematical work on the Enigma ciphers; 2. The French would maintain their intelligence contacts with their

agents ir Germany; and 3. The British would use their greater resources to design and construct at least sixty bombas to break the five-rotor Enigma. The Poles offered to help the British all they could; their mathematicians revealed all they knew and plans of the bombas were also supplied. But perhaps the most valuable gift was two examples of the 'AVA' copies of the German Enigmas, which arrived in Paris after the meeting. (Kahn, 1991, pp.79-81)

A French intelligence officer travelled to London on 16 August 1939, accompanied from Paris by a British Embassy's diplomatic courier, carrying a Polish AVA Enigma in the Diplomatic Bag. Meeting them off the boat train at Victoria Station was Menzies, then deputy and later head of MI5 (Kozaczuk, p.60). Sixteen days later Germany invaded Poland and the Second World War began (Whiting, p.41-2; Winterbotham, p.11).

Ironically the Poles, who had done more than any other nation to break the Enigma cipher, were to end up as the first nation to suffer from 'Blitzkrieg', the highly mobile war that Enigma made possible. Within days it was obvious to the Polish General Staff that the country was bound to be overrun; the Intelligence Section, including BS4, was evacuated from Warsaw and, by the final collapse at the end of September, had reached Romania, which was neutral at the time (Calvocoressi, p.57; Kozaczuk, pp.70-1). The journey proved rather treacherous because the train in which they travelled was attacked constantly from the air, and the Poles reluctantly decided to destroy their bomba, since there was a

distinct possibility of it falling into German hands and compromising the entire team. Eventually though, the whole prewar BS4, which included the vital three mathematicians, Rejewski, Rozycki and Zygalski, arrived safely at the French Embassy in Bucharest.

From there, the cryptanalysts immediately went on to Paris, with some, if not all, of the Enigma engineers from the AVA factory. By mid October 1939, the French had collected them together and established them at the Chateau de Vignolles (code-named 'Bruno'), in a small town some forty kilometers north of Paris (Kozaczuk, pp.82-3). Here, as team 'Z', they worked as a specialized decoding unit within the French's Service Renseignements (Ibid, p.118). A British Intelligence representative, Captain McFarlane, was also attached. Several replicas of the AVA Enigma were constructed. To preserve secrecy, the work was contracted out to light engineering works around Paris, no one concern being given enough of the machine to have any idea of its purpose. The final assembly was supervised by an engineer from the AVA factory.

The possession of the Enigma machine was of little value without the bomba, though team 'Z' continued the work of the mathematical analysis of intercepted Enigma radio traffic, which was very heavy at this point (Bennett, p.401). The team were helped when Alan Turing visited 'Bruno' in January 1940. Turing brought with him sixty complete sets of the 'perforated sheets'.

Each set consisted of twenty-six sheets with 1000 holes punched through; according to a Polish cryptanalyst, these were improved versions of the Polish originals, which Turing had made to cope with the five-rotor Enigmas (Kozaczuk, pp 96-8). No information has since been released as to how they were actually used, but once again, the ciphers were broken and the decodes were passed to Allied Intelligence until 14 June 1940. By that date, the Germans had broken through the Allied lines and were within a few kilometers of 'Bruno'. The Chateau de Vignolles was hastily evacuated with the most important files, the perforated sheets and the Enigma machines (Kahn, 1991, p.115)

To practically everyone, it seemed probable that the German forces would overrun the whole of France in the course of the next few weeks. Nevertheless, a French Intelligence officer managed to set up the codebreaking group in a similar operation in part of unoccupied France near Algiers, which was a French colony at the time. The building they were housed in was called Chateau Fouzes, but those 'in the know', referred to it by the code-name 'Cadix'. Additionally, the team was renamed 'Unit 300' in case any mention of team 'Z' was left at 'Bruno' (Kozaczuk, p.113). The French maintain that during their period of operation, that the cryptanalysts at 'Cadix' broke 673 German signals, mainly those sent to the Afrika Korps (Ibid, p.118); lacking a teleprinter circuit, these intercepts were sent to London via a radio transmitter which the British had delivered to Lisbon, where the French collected it.

The British end of the radio net was operated by Poles from a house in the North London suburb of Stanmore (Kahn, 1991, p.231).

Unit 300 continued its work until 8 November 1942, when the Germans occupied the whole of France. A few days later a German motorized column entered 'Cadix', but it was empty. The unit was now dispersed south; some-Rejewski and Zygalski among them-managed to escape over the Pyrenees into Spain, where clandestine organizations conveyed them, through Gibraltar, and onward to Britain (Kozaczuk, pp.135-6, 138-40). Some were not so lucky. Rozycki had gone down with the SS Lamoriciere when she was sunk in the Mediterranean earlier in 1942 (Kahn, 1991, p.117). Others were caught en route to Britain and were subsequently interrogated by the Gestapo. The chief engineer of 'Unit 300' was among those and eventually died in a German concentration camp. Not one of the captured Poles, though subjected to the most rigorous interrogation by the Gestapo, gave away so much as a hint that Enigma had been penetrated. Many eventually took their secrets to their unmarked graves in German concentration camps (Kahn 1991, p.117; Kozaczuk, p.211). With the dispersal of 'Unit 300', the Franco-Polish attack on Enigma came to an end; they had done a great service to the Allied cause, though in fact the major work on the German ciphers had already passed from France to England (Bennett, p.401).

Soon after the tripartite meeting in the summer of 1939, the British cryptanalysts of the Government Code and Cipher School

(mockingly called 'the Golf Club and Chess Society) had been evacuated to Bletchley Park where work began to solve the Enigma cipher. Bletchley Park was a rather large and ornate house with red bricks and timbered glass of the late Victorian style. There were twenty or more rooms in the two-storey house, entered through a pretentious porch. The mansion had spacious green lawns, a croquet lawn and a ha-ha, a sunken boundary fence that was invisible from the house and gave the illusion of unbroken space. This was a favorite place for the scientists to sit and eat their lunch (Winterbotham, p.13). The man eventually appointed to head this establishment was a naval officer, Commander Edward Travis, and a discreet recruiting campaign was implemented, largely among the mathematicians of Cambridge University (Whiting, p.131). Among the first recruits were Gordon Welchman and Alan Turing.

Turing was a brilliant scientist. In 1936 he had published a classic paper on 'computable numbers', now recognized as the theoretical basis of the modern computer (Kahn, 1991, p 92). He was most likely one of the British delegation who attended the tripartite meeting in 1939 and subsequently given complete details of the BS4 bomba. By the outbreak of war he was at Bletchley Park working on a British version of the 'bombe'. It is not clear how much it owed to its Polish prototype, but it seems to have been a big step forward, and Turing's contribution was considerable, for

he had two essential qualifications; he excelled at mathematics and mechanical engineering (Bennett, p.401-2).

Gordon Welchman, was also a Cambridge mathematician recruited (Kahn, 1991, pp.97-8). He received a letter asking him if, in the event of a war, he would be willing to serve his country He replied that he would and subsequently was requested to attend the Code and Cipher School in London for an initial indoctrination. Alan Denniston was head of the school at the time and asked Welchman to report to Bletchley Park on the first day of war, should it come

Upon the outbreak of war, Welchman arrived at Bletchley, and Denniston sent him to join Dilly Knox, then chief British cryptanalyst, Turing and others in a building known as 'the cottage', which was part of the stables behind the old mansion (Winterbotham, p.14). Other members of the group were on loan from the armed forces. Namely, J.H. Tiltman from the Army and a brilliant mathematician, Josh Cooper, who was borrowed from the Air Force. Three strange additions to the group were: Oliver Strachey, Benjamin Britten and Dick Pritchard. They had no military, mathematic or engineering skills, but excelled in the field of music theory. Winterbotham mentioned that it struck him how often the art of undoing other people's ciphers was closely allied to a brain which could excel both in mathematics and music (Winterbotham, pp.14-5).

By then, with the aid of the AVA machine, the group were beginning their work on the Enigma cipher. It is most likely that

additional copies had been made in Britain by that time. Due to the vital gift of the Polish machine, the complicated internal wiring of the five rotors was known, and it fortunately remained virtually unchanged throughout the war. The technique of the plugboard and the setting of the keys were known in principle, but apart from some decodes (supplied possibly by the French or Poles) no Enigma messages appears to have been deciphered at Bletchley before Welchman joined. At the time of his arrival, not much could be done in the area of actual cryptography. As a result, Knox didn't feel that he needed other cryptanalysts yet and sent him to work alone on radio call signs and 'discriminates'. As things turned out, this accidental move was to prove highly beneficial. Welchman quickly realized that the radio call signs were in effect the addresses of the sender and recipient and the 'discriminates', as Denniston called them, were the codes that the Germans used to indicate the vital keys in which that particular message had been enciphered. It now dawned on Welchman that they weren't really dealing with a cryptographic problem, but rather, they were dealing with the entire communications system that the Germans had developed for their Blitzkrieg (Kahn, 1991, pp 98-9). Here were the commanders talking to each other, reporting and getting their instructions from High Command. The radio call signs now were viewed as actual military units, not a radio station; and the 'discriminates' made it possible to distinguish between different

kinds of traffic that was being sent (Kahn, 1983, p.10; Kozaczuk, pp. 158-9, 295-7).

Although the British had yet to break Enigma, a simple analysis of the traffic which Welchman undertook with the help of the Navy's 'Y' intercept stations revealed the scope and complexity of the German armed forces' signals organization, which was by far the most elaborate system of military communications in the world in 1939. Without a quick, easy-to-operate and secure encoding system, radio could not be used; without radio there could be no Blitzkrieg. It was as clear as that. The only alternative to Enigma that could offer total security would have been the 'one-time pad', and as stated earlier, this was not suitable because of the much longer time required for encoding and decoding. Additionally, the volume of enciphered radio traffic at the time made it logistically impossible to supply the needs of the German forces with disposable one-time pads (Winterbotham, p.9).

Therefore, Enigma was the solution. Its penetration was now more important than ever. Welchman plotted the movements of units from their call signs and soon realized that once the secrets of the five-letter groups that formed the texts of the intercepted messages were broken, a huge organization, equivalent in numbers to the German army's Signals Corps, would be needed to deal with the landslide of coming Enigma intercepts. The height of Cryptanalysts' work now reach a level unheard of (Kozaczuk, pp.297-8).

With a new organizational plan in place to prepare for the up-in-coming onslaught of intercepts, the group at Bletchley got permission to start recruiting immediately. They took on a variety of skills: radio operators to man the intercept stations; females from the Woman's Royal Naval Service (WRNS) to act as decoding clerks; foreign language specialists in German, Japanese, and Italian, mechanical and electrical engineers, statisticians, theoreticians, mathematicians and intelligence experts. A complete organization that would eventually number 10,000 men and women who were sworn to complete secrecy (Bennett, pp 403, 406-7; Calvocoressi pp 3.45, Kahn, 1991, p 231, Kozaczuk, p 159)

Within a few weeks the basic organization was ready and waiting for the moment when the cryptanalysts had broken the five-rotor Enigma ciphers. This was an intimidating prospect. The military Enigma used by the Army and Luftwaffe, had 10 to the twenty-first power of possible initial settings of the machine; for the Navy's Enigma, there existed the use of four operational rotors out of a possible eight, the figure would be 10 to the twenty-third power of possible settings (Bennett, p.402). As a result, even the possession of an Enigma machine was of little help.

Nevertheless, the codes were broken. The principal aid was the bombe, which was a dangerous cover name to choose, since had the Germans discovered it they could have concluded that the atom bomb was being developed at Bletchley, which was well within their bombing range. Apart from the name, it is not documented as

to how much similarity that the British bombe had with the Polish prototypes. It is, however, reasonable to assume that the British bombe worked very much more quickly than the Polish original and that the British machines were much larger objects (Kahn, 1991, pp.230-3). Dr Good, another mathematician who worked at Bletchley, stated that they were about ten feet high. These objects were most likely the "bronze-colored Eastern goddesses' to which Winterbotham refers in The Ultra Secret (Winterbotham, p.15). The bombes were not electronic, but rather electro-mechanical. In a real sense they were Enigma machines in reverse, but far more complex by simulating the three operational rotors many times over (Bennett, p.401). They had a plugboard on which a 'menu' was selected; this menu was really a set of electro-magnetic instructions to the bombe which reduced the number of possible initial states of the Enigma machine from 10 to the twenty-first power, to a much lower, more attainable figure. The menus were drawn up in Hut 6 for the Army and Air Force, and in Hut 8 for the Navy. The menu selection was aided greatly by the Germans themselves; indeed, without that aid early on, the task could have been impossible.

It should be explained that there were very large numbers of Enigma machines issued to the German forces, a figure of 200,000 has been mentioned, and they were in daily use encoding a tremendous volume of traffic, which meant that the messages contained the same phrases time after time. Examples of repeating

phrases are: 'To Officer Commanding', 'By order of the Fuhrer', or even 'Heil Hitler'. Such repetition is 'the fuel for the fire' to cryptanalysts since, once decoded in one cipher, they provide 'keys' to others (Kahn, 1991, p.69). Weather reports also helped, for the European weather systems tend to move from west to east, thus the British knew in advance the sort of meteorological forecasts the German's would send, particularly to the Luftwaffe (Kahn, 1991, pp.190,229).

German cipher clerks unwittingly helped in several ways. Often a headquarters signals officer would have to send in order to several units, each on a different 'net', each with its individual Enigma keys. The army used many of these nets. Incredibly, the men operating the machines would send an identical message enciphered in different keys (Kahn, 1991, pp.62-3). Thus, when Bletchley broke one of these they had a plaintext equivalent for all the other settings, not only for that particular message but for all subsequent ones, until the 'ground keys' were chained again. Additionally, the method of setting up the keys invited carelessness which offered valuable help to the codebreakers. As stated earlier, the operators had to think up three random letters to be tapped out twice on the machine; many used 'XYZ' or even 'ABC' or, contrary to regulations, the same three letters; some continually used their own initials or those of a girl friend, over and over again. The units of these men would become known from their radio call signs and Bletchley's Hut 6 would soon have the key

for the day (Bennett, p.401; Calvocoressi, p.34; Kahn, 1991, p.112; Kozaczuk, p.42). There were other common practices which helped. For example, 'Q' is a letter little used in German, 'CH' on the other hand is very common and many units used 'Q' for 'CH', which made decipherment much easier. Moreover, there were no punctuation marks on the Enigma keyboard, so 'YY' was often used for stop.

The cryptanalysts also relied heavily on 'females' which were often present in the keys. Suppose SOXSOX were the 'random' letters an operator had used and they had encoded as WRTWQL; here a 'W' appears twice. When a letter appeared twice in the key cipher it was known as a female. If thirty or so of these females were received in the same key, the bombe's menu could be plugged up with a fair chance of decoding the messages (Kahn, 1991, p.70). The Poles were the first to discover the technique, but the term was coined at Bletchley and originally meant an alignment of the holes on the perforated sheet which was used on the light tables. Turing, as has been noted, improved on the original light-table technique and adapted it to the bombe.

The Enigma machine itself helped. Because it 'reflected' the pulses through its three rotors, it could never encipher a letter as itself (Kahn, 1991, p.113) This defect was also exploited by the British, who would send out an aircraft to destroy a known lightbuoy, one which marked a safe channel for U-boats to pass through perhaps. Then radio interception stations would be alerted to listen particularly for traffic from the relevant command; soon

a radio message would be sent warning the U-boats, and the cryptanalysts would be fairly certain that the phrase 'the lightbuoy is gone' would appear in the text. Then, by comparing the plaintext German phrase with the cipher groups, they would look for a point in the message where none of the plaintext letters appeared in the cipher. Because of Enigma's inability to encode a letter as itself, that section would, with luck, be the cipher equivalent of the phrase (Kahn, 1991, pp.95-6) When that sort of information was available, it would be set up on the plugboard behind the bombe as part of the menu.

The bombes consisted of twenty-five to thirty sets of three rotors, which were wired in exactly the same way as the Enigma machines and also had the twenty-six letters of the alphabet engraved on their circumference. Each set of three rotors was arranged vertically, one above the other, the top one representing the first rotor of the Enigma, the middle the second and the bottom the third (Kahn, 1991, pp.99-100). They were color-coded and were changed by the WRNS operators on instruction from Hut 6 or 8. The cryptanalysts could ascertain which three of the five rotors were in use, probably by some type of mathematical analysis of the key cipher or possibly from the presence of 'females' in the key.

The plugboard had many rows of jacks like a telephone exchange, except that the jacks were arranged in lines of twenty-six and each was labelled with a letter of the alphabet. The plugs were again, standard telephone exchange equipment, which enables

the menu to be set up (Kozaczuk, p.20). Once the menu was plugged up and the correct rotors put in place, the machine would be switched on to commence its search.

The rotors were electrically driven and clicked round interminably, mimicking the Enigmas When the first wheel had completed one revolution of twenty-six letters, the second one below it moved forward one letter, when this had completed its twenty-sis letters, then the third wheel started its slow rotation On completion of the third twenty-six letters, that trio of rotors would have tested no fewer than twenty-six to the third power, offering more than 17,000 possible combinations (Calvocoressi, p.34). At the same time, the other thirty or so sets of rotors would be doing the same thing. However, when a set of rotors found the letter substitution that the 'menu' had programmed it to find, it would throw a switch; when all the rotors had completed their programme and the enciphered message had become decoded into its plaintext, the machine would switch off and the and the WRNS who operated it would report a 'stop' (Kahn, 1991, p.97). This could take anywhere from ten minutes to ten hours

It should be stated that the bombes were not, in themselves, decrypting machines; their function was to recreate the state of the enciphering Enigma (Kozaczuk, pp.53-4). If it was a 'correct stop', and not all were, then the message would appear as plaintext and the signal of 'reds up' or 'greens up' would be sent on to Intelligence officers in Hut 3. The colors being messages to

indicate to Intelligence, the anticipated importance of deciphered messages (Kozaczuk, p.293). The Enigmas which were used at Bletchley were British built and had the advantage over the German originals in that they printed out the decodes on strips of gummed paper, like a telegram, which were then stuck to a sheet of paper and sent to the intelligence huts for analysis.

It is not known how many bombes there were, some were at Bletchley, others were in the 'outstations' scattered around the countryside, usually in large country houses At the these houses, the machine rooms were staffed by WRNS who had volunteered for service, then sent to Bletchley or one of the outstations, where they were required to operate the bombes on an eight hour shift, for the duration of the war. There were three shifts each in the twenty-four hour day (Kahn, 1991, pp.231-2).

The actual work of the cryptanalysis was conducted out of Huts 6 and 8 at Bletchley. It was here that the menu was prepared and also where the plugboard of the Enigma was solved This board was responsible for a very large percentage of the 10 to the twenty-first power figure of combinations but was apparently solved by another of Turing's machines (Ibid, pp.94-5, 97).

The first decodes at Bletchley were made sometime around April of 1940 during the Norwegian campaign. From that time the quality and number of intercepts rose steeply and by May, when the Battle of France began, the codebreakers in Hut 6 were reading a significant portion of the Enigma traffic. However, this is not to

say that all the signals were broken; some were only partially solved and others not at all. Certain keys took longer to recover, so a system of priority was used. In this instance, the traffic which, from its origin as revealed by direction-finding and the call signs used, was considered to be the most important was dealt with first, and given the color-code red (Bennett, p.405).

By mid May, the effectiveness of the Germans' Blitzkrieg was all too clear. German tanks were continuing their advance across France , driving at top speed with commanders, in Signal Corps trucks, co-ordinating close-support attacks on the French troops with Stuka dive-bombers; and it was the Enigma machine which made it all possible.

The group at Bletchley intercepted and broke many of the enciphered radio messages as France was being overrun, but to the men in the Huts there was little excitement in their accomplishments, for the scenes revealed were rather grim. The Allied forces were clearly unable to defend against the straight on advance of the German army. In a military sense, the battle was a defeat. Nevertheless, for the cryptanalysts in the wooden Huts at Bletchley, however bitter, it was still a victory; for the first time in years, codebreakers had been able to influence the tactical response of a battle.

The intelligence analysis of Enigma was accomplished in other huts at Bletchley, mainly Hut 3, where skilled interpreters pieced the information together (Bennett, p.403; Calvocoressi,

p.55). Nothing was too trivial; everything, however small, was collated and filed in a huge card index containing hundreds of thousands of names, units, postings, supply requisitions, details of transfers, promotions, or even courts martial (Bennett, p.408-9). A transfer of one or more Air Force pilots could reveal an impending attack, possibly revealing the target. The card index grew until it was virtually the archives of the entire German Command structure. As the intelligence mounted, a special organization was developed to handle it. It was distributed under the name 'Ultra' and Special Liaison Units (SLUs) were formed by the RAF Intelligence officer, Captain Winterbotham (Calvocoressi, p.60; Winterbotham, pp.20-1).

As the war progressed, the organization centered at Bletchley grew, and more and more German radio signals were intercepted for the codebreakers. The actual radio interceptions were made at several stations as far apart as northern Scotland, the Midlands, South Whales, and on the east coast. Many of the stations in the small country homes, had their array of directional rhombic aerials hidden in foliage around the country side (Calvocoressi, pp 41-3) At the time, approximately 600 girls of the WRNS worked in shifts around the clock taking down the faint morse signals from Germany and Occupied Europe. The sets were mainly communication receivers with highly selective crystal to enable the operators to cut out interfering signals. It was a tedious job, for the signals that were copied, day after day, with the greatest possible

accuracy, were to the operators a meaningless series of five-letter groups. Very important signals would be received on several sites as far apart as possible, in the hope that if one radio signal was fading or jammed by interference, it might be clear at another location. This also allowed cross matching of identical signals to check for accuracies and possible discrepancies. The intercepted messages were sent by dispatch rider or teleprinter over secure land-lines to Bletchley (Bennett, p.403).

The Ultra messages that were intercepted undoubtedly effected the conduct of the war. The Battle of France, as mentioned earlier, was one; the Battle of Britain, according to Winterbotham, was another (Whiting, p.47). He recalled talking to Air Marshal Dowding personally after the Battle of Britain in which Dowding said that it was the greatest help to him (through Ultra) to know what Reichsmarschall Goering's policy was, because as Goering got more and more desperate, he gave orders to his fighter squadrons that they must bring the RAF fighters up to battle. The Lufwaffe then sent greater and greater formations of fighters over airfields to draw the RAF but Dowding only used a squadron or so to meet these attacks. The maneuver by the Luftwaffe failed, but by the beginning of September 1940 the strain on the RAF was becoming unbearable. Then, a deciphered signal came to Dowding, which told the Lufwaffe bombers to change from attacking the fighter airfields to the city of London. It was that change of policy

by Goering which Dowding credits to the survival of the RAF (Winterbotham, pp.44-7, 54).

Air Marshal Dowding was more than glad to utilize the Ultra intelligence. Much later in the war, the hard-nosed American General, Patton, was a great user of Ultra; he, like the German generals, had his signals truck travelling with his tanks, the difference being that his truck was receiving the decodes via Bletchley (Winterbotham, p.98). His British arch-rival, Field Marshal Montgomery, on the other hand, did not care for Ultra and at times ignored its intelligence (Winterbotham, pp.75, 78).

Some of the most exciting successes of Ultra were during the North African campaign, particularly with decoding of messages giving details of the routes of Rommel's Afrika Korps supply ships which were as a consequence sunk by the Royal Navy in large numbers (Bennett, pp.411-12). It has been said that the conditions were so favorable for the codebreakers during the North African campaign that at times the Allied Armies in Cairo had the Enigma telegrams before Rommel himself (Winterbotham, pp.25, 69, 71).

Ultra was also instrumental in confirming that Operation Sea-Lion, Hitler's plan to invade south-east England, was definitely off. Winterbotham immediately informed Churchill of this after the group at Bletchley deciphered a message from Berlin, giving orders to dismantle the aircraft loading ramps on a certain Dutch

airfield, which was probably to have been the staging site (Whiting, p.47,131).

Although the Ultra intelligence that was flowing from the Enigmas of the Army and Air Force was readily accessible, it was a different story with the German Navy. Possibly from their experiences during World War One, the German Navy were much more security-conscious than the other services, being aware that radio was the only possible link with their fleets at sea. So from the outset they had their own version of Enigma ciphers, known generally as 'Key M'. There were in fact some thirteen different ciphers in use, of which the most important from the Allied point of view was Hydra, the cipher used by the operational U-boats in the North Atlantic (Calvocoressi, p.86; Kahn, 1983, p.111; Kozaczuk, p.201).

The Enigma machines used by the U-boats had, as noted earlier, four rotors to be chosen from eight, giving the cryptanalysts a figure of ten to the twenty-third power to cope with. German Naval cipher clerks were far better disciplined and made fewer mistakes. For a year between 1940 and the summer of 1941, Bletchley failed to break Hydra. Patrick Beesley, who served in Naval Intelligence in the U-boat tracking room at the Admiralty in London during the war, has recounted in his book, Very Special Intelligence, how cipher materials and spare rotors were captured in 1941 from three German armed trawlers. The material was described, as usual, as 'of inestimable value', but the men in Naval

Hut 8 had still not solved Hydra when, on 8 May 1941, U-boat 110 was captured following an battle off Greenland with the Royal Navy corvette Aubrretia and the destroyers HMS Bulldog and Broadway (Kahn, 1983, p.111). A boarding party managed to recover the Enigma machine, its rotors and the current cipher books intact form the U-boat; a fact which pleased the Admiralty since the U-boat sank, from existing damage, while under tow to Iceland. Beesley states that this chance-discovery enabled Bletchley to penetrate Hydra at last.

Hydra was eventually replaced by another U-boat cipher, 'Triton', which, with the aid of improved bombes and the experience gained with Hydra, was also broken by April 1943 (Kahn, 1991, pp.185-6, 205, 216). The result was that the vital convoys could be rerouted clear of the 'wolf packs' of U-boats. The penetration of Triton also enabled the hunting down of Germany's 'milch cows', the fuel tankers for U-boats, to such an extent that every single one of them was sunk (Ibid, p.274).

Enigma was not the only cipher machine used by the Germans; there were others. One such machine was known in Germany as the Geheimschreiber, secret-writing machine (Kahn, 1983, p.52). It was only used for the highest grades of traffic, from the German Foreign Office to keep in touch with embassies in still neutral countries or for Hitler's directives and broad strategic plans to distant commands (Ibid, p.111-12). The Enigma ciphers were not regarded as secure enough for this purpose. The essence of Enigma

was its use tactically where speed was of the essence. The Germans had considered that the problems of solving the ciphers, though not totally impossible, would take so long that by the time they had been broken the information recovered would be militarily useless. Foreign Office dispatches and strategic plans, on the other hand, were of far longer relevance and importance.

Fortunately the scientists at Bletchley were also successful at penetrating this cipher machine. What made there work successful was the invention and design of the first electronic computer (Kahn, 1983, p.117). The name given to the first computing machine at Bletchley was the Colossus (Kozaczuk, pp.162-63). By 1943, began producing results almost immediately. The exact nature of Colossus' function has not been revealed but the intelligence obtained was considerably vital and was also, for that reason, given the 'Ultra' priority (Cave Brown, pp.276-77).

With the official release of Ultra intelligence, the extent of the Allied penetration of the German command structure may now become more clear. The influence of the cryptanalysts and other scientists at Bletchley on the conduct of the war was profound. At the vary least it must have saved the lives of many Allied soldiers. It had to be used with great caution however; during the war the users of 'Ultra' were ordered never to take action based on the intelligence that could not have been attributed to other sources such as reconnaissance or interrogation of prisoners (Bennett,

pp.413-14). If the Germans realized that there messages were being decoded on such a broad scale, could have led to the discontinuance of Enigma and consequently a loss in Bletchley's service.

Thus the bombes and Colossus continued to provide the German secrets to the last day of the European war, when they fell silent for the first time in over four years. The cryptanalysts and mathematicians went back to their universities, picking up on the research they abruptly abandoned at the onset of the War; some scientists went into the emerging field of computers.

The work accomplished and the technologies advanced by mobilizing scientists from various fields of study and from multiple countries, leaves an indelible mark. If the Official history of Ultra is ever published, then a true assessment can be made. It is quite possible that an entire revision of assumptions and conclusions about World War Two is needed (Whiting, p.131). Since Bletchley had intercepted and deciphered much of the enemy's wireless cryptography throughout most of the war, there is no escaping a reexamination of almost all the important decisions made by Western statesman and generals. The matter of who knew what and when obviously would be of paramount importance (Laqueur, p.18; Bennett, p.416). Nevertheless, it is an inescapable fact that assembling an intellectual-pool of scientists to solve a problem or to advance a technology can be of inestimable value.

Works Consulted

Beesly, Patrick. Room 40. Harcourt Brace Jovanovich Publishers: San Diego, 1982.

Beesly, Patrick. Very Special Intelligence. Harcourt Brace Publishers: New York, 1978.

Bennett, Ralph. Ultra and Mediterranean Strategy. William Morrow and Company, Inc.: New York, 1989.

Calvocoressi, Peter. Top Secret Ultra. Pantheon Books: New York, 1980.

Cave Brown, Anthony. The Last Hero: Wild Bill Donovan. Times Books: New York, 1982.

Dunlop, Richard. Donovan: America'a Master Spy. Rand McNally and Company: Chicago, 1982.

Hyde, Montgomery H.. Room 3603. Farrar, Straus and Company: New York, 1976.

Jones, R.V.. Most Secret War. Coronet Books: Hodder and Stoughton, 1979.

Kahn, David. The Codebreakers. Weidenfeld and Nicolson Publishers: London, 1967.

Kahn, David. Kahn on Codes. Macmillan Publishing Company: New York, 1983.

Kahn, David. Seizing The Enigma. Houghton Mifflin Company: Boston, 1991

Kozaczuk, Wladyslaw. Enigma. University Publications of America, Inc.: New York, 1984.

Lagueur, Walter. "The Untold Story of World War Two." The New Republic. Vol. 185: pp. 18-20, 14 October 1981.

Lewin, Ronald. The American Magic. Farrar Straus Giroux: New York, 1982.

Roosevelt, Kermit. War Report of the O.S.S.. Walker and Company: New York, 1976.

Stevenson, William. A man Called Intrepid. Ballantine Books: New York, 1976.

Time. "An Uncrackable Code." Vol. 112: pp. 55-57. 3 July 1978.

Van Der Rhoer, Edward. Deadly Magic. Charles Scribner's and Sons: New York, 1978.

Whiting, Charles. The Spymasters. Saturday Review Press: New York, 1976.

Winterbotham, F.W. The Ultra Secret. Harper and Row, Publishers: New York, 1974.